Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A computer-implemented method for a secure transaction ~~process~~, comprising:

generating a first key from a user-supplied unencrypted password,

encrypting the user's password with the first key,

creating a user record, and

storing the encrypted password in the user record.

2. (Currently Amended) The computer-implemented method ~~process~~ of claim 1, further comprising

upon user login, generating a second key from a would-be user's password using the same algorithm used to generate the first key from the originally supplied unencrypted password,

retrieving the corresponding user record,

decrypting the encrypted password in the user record using the second key, and

comparing the decrypted password with the would-be user-supplied password to see if they match.

3. (Currently Amended) The computer-implemented method ~~process~~ of claim 2, further comprising

if the decrypted password and user-supplied password match, creating a temporary session record and storing the second key in the session record, otherwise aborting the user login.

4. (Currently Amended) The computer-implemented method ~~process~~ of claim 3, further comprising

encrypting other sensitive user data using the first key and storing the encrypted data in the user record, and

during a session wherein a session record has been created, using the second key stored in the session record to decrypt other encrypted information stored in the user record for use in carrying out some desired action.

5. (Currently Amended) The computer-implemented method ~~process~~ of claim 1, further comprising

generating a public/private key pair,

storing the public key on an application server and the mating private key only on another server,

encrypting the original user-supplied unencrypted password with the public key and storing the public-key encrypted password on the application server, and

fetching the private key from the other server and using it to decrypt selected information on the ~~one~~ application server.

6. (Currently Amended) The computer-implemented method ~~process~~ of claim 5, ~~further~~ wherein the other server is a secure off-site server.

7. (Currently Amended) A computer-executable program residing on a computer, the execution of the program causing the computer to: ~~secure transaction process, comprising~~

generate ~~generating an~~ a first, encryption key from user-supplied identification data,

encrypt ~~encrypting~~ the user's identification data with the first key,

create ~~creating~~ a user record, and

store ~~storing~~ the encrypted identification data in the user record.

8. (Currently Amended) The ~~process~~ computer-executable program of claim 7, further causing the computer to ~~comprising~~

upon user login, generate ~~generating~~ a second key from a would-be user's identification data supplied at login using the same algorithm used to generate the first key from the originally supplied unencrypted identification data,

retrieve ~~retrieving~~ the corresponding user record,

decrypt ~~decrypting~~ the encrypted identification data in the user record using the second key, and

compare ~~comparing~~ the decrypted identification data with the would-be user-supplied identification data to see if they match.

9. (Currently Amended) The ~~process~~ computer-executable program of claim 8, further causing the computer to ~~comprising~~

if the decrypted identification data and user-supplied identification data match, create ~~creating~~ a temporary session record and storing the second key in the session record, otherwise aborting the user login.

10. (Currently Amended) The ~~process~~ computer-executable program of claim 9, further causing the computer to ~~comprising~~

encrypt ~~encrypting~~ other sensitive user data using the first key and storing the encrypted data in the user record, and

during a session wherein a session record has been created, use ~~using~~ the second key stored in the session record to decrypt other encrypted information stored in the user record for use in carrying out some desired action.